

REMARKS

Applicants respectfully request reconsideration of this application as amended.

By this amendment, Claim 1 has been amended to include the features of Claims 2-4 with Claims 2-4 being cancelled. Furthermore, the features of cancelled Claim 4 have been included in amended Claims 8 and 10. Claim 9 is cancelled.

Applicant would like to bring to the attention of the Examiner, that while the Office Action Summary indicates that Claims 1-7 are pending in the application, by virtue of the Preliminary Amendment filed on June 28, 2001 (copy enclosed), Claims 1-11 are pending.

Independent Claim 1 has been amended to recite, *inter alia* . . . k unpredictable values wherein k is greater than 2. This feature is at least supported by the description (page 5, lines 4-7: "Advantageously, said values (d_1, d_2, \dots, d_k) are obtained in the following way: (k-1) values are obtained by means of a random generator; the final value is obtained from the difference between the secret exponent and the (k-1) values"). It is recited, "(k-1) values are [. . .]". Since the plural form is used in this sentence, (k-1) is greater than 1. Consequently, k is greater than 2.

Claims 8 and 10 have also been amended to recite that k is greater than 2.

Claims 1-7 are rejected under 35 U.S.C. 102(e) as anticipated by the '658 patent to Kocher. Kocher is directed toward an apparatus for securing cryptographic devices against attacks involving external monitoring and analysis. Kocher also teaches a leak resistant cryptographic operation that modifies or updates secret key material in a manner designed to render useless any information about the secrets that may have leaked from the system. Further, Kocher discloses methods of leak-proof implementations for symmetric authentication RSA.

However, Kocher does not teach or suggest a method for protecting an electronic system using a secret exponent (d) and breaking down the exponent (d) into a plurality of k unpredictable values (d_1, d_2, \dots, d_k), wherein k is greater than 2. In contrast, Kocher only teaches the breakdown (d) into two halves such that ($d_1 + d_2 = d$). (See, for example, Kocher column 16, line 30). Kocher does not teach or suggest the breakdown of (d) into more than two values whereas amended Claim 1 specifically states "breaking down said secret exponent (d) into k unpredictable values . . . wherein k is greater than 2.

Moreover, Kocher actually teaches away from this feature in that Kocher includes an additional step of computing a random integer “ r ” (wherein “ r ” must be lower than the greater half), subtracting “ r ” from the greater half and adding “ r ” to the lower half in order to obtain a new value of d_1 and d_2 . Thus, in Kocher, the methodology prohibits the breaking down of (d) into more than two values.

Furthermore, Applicant respectfully submits that Claim 1 includes the feature of at least one of said ($k-1$) values has a length at least equal to 64 bits, the sum of which is equal to said secret exponent. The Office Action asserts this feature is disclosed in Kocher, column 4, lines 58-60. However, in contrast, Kocher only discloses a variable (L) that defines “a number of bits of useful information about cryptosystem’s secret that are revealed per operation” (see column 3, lines 16-30). Kocher’s value (L) does not correspond to the values (d_1, d_2, \dots, d_k) as set forth in the claims which define fractions of (d). Furthermore, Kocher further recites that “ L_{MAX} must be chosen conservatively” and equal to at most 64 bits ($L_{MAX}=64$) and not at least to 64 bits as recited in independent Claim 1. (See, for example, column 4, line 60 of Kocher).

Still further, Kocher does not teach or suggest the deriving or obtaining features of Claim 1, but only rather eludes to a method of splitting open (d) into two integers such that ($d_1 + d_2 = d$).

At least based on the above distinctions, Applicants respectfully submit that Claim 1 is patentably distinguishable from the Kocher reference. The claims that depend therefrom are also patentably distinguishable based on the above and the feature(s) recited therein. For example, and with regard to Claim 7, which recites using the Rabin algorithm, this feature is not anticipated by the asymmetric method for protecting calculations and in particular the Diffie-Hellman method disclosed on column 15, lines 22-27 of Kocher as referenced by the Office Action. There is simply no teaching or disclosure of the Rabin algorithm in Kocher.

Accordingly, Applicants respectfully submit the application is in condition for allowance. A prompt and favorable Notice of Allowance is respectfully requested.

The Commissioner is hereby authorized to charge to deposit account number 50-1165 (T2146-907343) any fees under 37 CFR § 1.16 and 1.17 that may be required by this paper and to credit any overpayment to that Account. If any extension of time

is required in connection with the filing of this paper and has not been separately requested, such extension is hereby requested.

Respectfully submitted,

JHV:jab

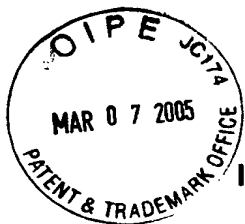
Miles & Stockbridge P.C.
1751 Pinnacle Drive, Suite 500
McLean, Virginia 22102-3833
(703) 903-9000

By: _____

Edward J. Kondracki
Reg. No. 20,604

Jason H. Vick
Reg. No. 45,285

March 7, 2005



COPY

T2146-907343-US 3857/BC(PCT)

IN THE UNITED STATES DESIGNATED/ELECTED OFFICE (D.O./E.O./US)

Applicant: Louis GOUBIN

International
Application No.: PCT/FR00/02978

International
Filing Date: 26 October 2000

U.S. Serial No.: To be Assigned

U.S. Filing Date: June 28, 2001

For: **SECURITY METHOD FOR A CRYPTOGRAPHIC
ELECTRONIC ASSEMBLY BASED ON MODULAR
EXPONENTIATION AGAINST ANALYTICAL ATTACKS**

McLean, Virginia

PRELIMINARY AMENDMENT

Honorable Commissioner of Patents
and Trademarks
Washington, D.C. 20231

Sir:

Please amend the subject application, filed concurrently herewith, as
indicated below:

IN THE TITLE:

Please cancel the title in its entirety and substitute the following new title:

**-- METHOD FOR PROTECTING AN ELECTRONIC SYSTEM WITH MODULAR
EXPONENTIATION-BASED CRYPTOGRAPHY AGAINST ATTACKS
BY PHYSICAL ANALYSIS--**

IN THE SPECIFICATION:

After the title and before the first paragraph on page 1 at line 5, insert the
following heading at the left-hand margin:

--FIELD OF THE INVENTION--;

Page 1, at line 13, insert the following heading at the left-hand margin:

--BACKGROUND OF THE INVENTION--;

Page 7, at line 13, insert the following heading and sentence:

--BRIEF DESCRIPTION OF THE DRAWING

Fig. 1 is a representation of a smart card.—

Page 7, delete the two paragraphs beginning at line 15 and ending at line 33 in their entirety and insert the following new paragraphs. (Paragraphs showing the changes using underlining and bracketing are included as an attachment at the end of this Preliminary Amendment).

--The invention can be implemented in any electronic system performing a cryptographic calculation involving a modular exponentiation, including a smart card 8 as shown in Fig. 1. The chip includes information processing means 9, connected on one end to a nonvolatile memory 10 and a volatile working memory RAM 11, and connected on another end to means 12 for cooperating with an information processing device. The nonvolatile memory 10 can comprise a non-modifiable ROM part and a modifiable part constituted by an EPROM, an EEPROM or a RAM of the "flash" type, or FRAM, (the latter being a ferromagnetic RAM)), i.e., having the characteristics of an EEPROM but with access times identical to those of a standard RAM.

For the chip, it is possible to use, in particular, a self-programmable microprocessor with a nonvolatile memory, as described in U.S. patent No. 4,382,279 assigned to the assignee of the present invention. In a variant, the microprocessor of the chip is replaced, or at least supplemented, by logical circuits installed in a semiconductor chip. In essence, such circuits are capable of performing calculations, including authentication and signature calculations, as a result of hard-wired, rather than microprogrammed, electronics. In particular, they can be of the ASIC ("Application Specific Integrated Circuit") type. Advantageously, the chip is designed in monolithic form.--

Page 8, after line 22, insert the following new paragraph:

--While this invention has been described in conjunction with specific embodiments thereof, it is evident that many alternatives, modifications and variations will be apparent to those skilled in the art. Accordingly, the preferred embodiments of the invention as set forth herein, are intended to be illustrative, not limiting. Various changes may be made without departing from the true spirit and full scope of the invention as set forth herein and defined in the claims.—

IN THE CLAIMS:

Please amend claims 1 – 7, and add new claims 8-11. The claims that follow are a complete set of “clean” claims. The original claims 1-7 marked up to show the changes with underlining and bracketing are included as an attachment to this Preliminary Amendment:

1 1. (Amended) A method for protecting an electronic system
2 implementing a cryptographic process involving calculation of a modular
3 exponentiation of a quantity (x), said modular exponentiation using a secret
4 exponent (d), comprising breaking down said secret exponent (d) into a plurality
5 of k unpredictable values (d_1, d_2, \dots, d_k), the sum of which is equal to said secret
6 exponent.

1 2. (Amended) A method according to claim 1, characterized in that
2 said unpredictable values (d_1, d_2, \dots, d_k), are obtained by:

- 3 a) deriving $(k-1)$ values by means of a random generator; and
4 b) taking the difference between the secret exponent and the $(k-1)$
5 values to derive a final value.

1 3. (Amended) A method according to claim 1, wherein calculation of
2 the modular exponentiation is performed by:

- 3 a) raising the quantity (x) by an exponent comprising said value to
4 obtain a set of results for each of said k values and
5 b) calculating a product of the results obtained in step a).

1 4. (Amended) A method according to claim 1, wherein at least one of
2 said $(k-1)$ values is obtained by means of a random generator and has a length

3 at least equal to 64 bits.

1 5. (Amended) Utilizing the method according to claim 1 in a smart
2 card comprising information processing means.

1 6. (Amended) Utilizing the method according to claim 1 for protecting
2 a cryptographic calculation process using the RSA algorithm.

1 7. (Amended) Utilizing the method according to claim 1 for protecting
2 a cryptographic calculation process using the Rabin algorithm.

Please add the following new claims:

1 --8. (New claim) A method for protecting an electronic system
2 implementing a cryptographic process involving calculation of a modular
3 exponentiation of a quantity (x), said modular exponentiation using a secret
4 exponent (d), comprising breaking down said secret exponent (d) into a plurality
5 of k unpredictable values (d_1, d_2, \dots, d_k), the sum of which is equal to said secret
6 exponent; obtaining said unpredictable values (d_1, d_2, \dots, d_k) by deriving ($k-1$)
7 values by means of a random generator; by raising the quantity (x) by an
8 exponent comprising a final value and obtaining a set of results for each of said k
9 values and calculating a product of the set of results and taking the difference
10 between the secret exponent and the ($k-1$) values to derive the final value.

1 9. (New Claim) A method according to claim 8, wherein at least one of
2 said ($k-1$) values is obtained by means of a random generator and has a length
3 at least equal to 64 bits.

1 10. (New Claim) A smart card adapted to protect an electronic system
2 comprising means for implementing a cryptographic process involving calculation
3 of a modular exponentiation of a quantity (x), said modular exponentiation using
4 a secret exponent (d), comprising breaking down said secret exponent (d) into a
5 plurality of k unpredictable values (d_1, d_2, \dots, d_k), the sum of which is equal to
6 said secret exponent, means for obtaining said unpredictable values ($d_1, d_2, \dots,$
7 d_k) by a random generator for deriving ($k-1$) values and means for taking the

8 difference between the secret exponent and the $(k-1)$ values to derive a final
9 value.

1 11. (New Claim) A smart card according to claim 10, wherein calculation
2 of the modular exponentiation is performed by:

- 3 a) raising the quantity (x) by an exponent comprising said value to
4 obtain a set of results for each of said k values and
5 b) calculating a product of the results obtained.--

IN THE ABSTRACT:

Please delete the Abstract at page 11 in its entirety and substitute the following new Abstract.

--ABSTRACT

The invention concerns a method for protecting an electronic system implementing a cryptographic calculation process involving a modular exponentiation of a quantity (x), said modular exponentiation using a secret exponent (d), characterized in that said secret exponent is broken down into a plurality of k unpredictable values (d_1, d_2, \dots, d_k), the sum of which is equal to said secret exponent.--

REMARKS

This Preliminary Amendment is filed to insert headings to conform the application to U.S. practice and to correct informalities in the specification, claims and abstract resulting from a literal translation of the French text.

Early action on the merits is earnestly solicited.

Respectfully submitted,

MILES & STOCKBRIDGE P.C.

Date: June 28, 2001

By: 

Edward J. Kondracki
Registration No. 20,604

1751 Pinnacle Drive – Suite 500
McLean, VA 22102-3833
Tel.: 703/903-9000
Fax: 703/610-8686

The following are the two paragraphs on page 7 beginning at line 15 and ending at line 33 showing the changes made using underlining and bracketing:

The invention can be implemented in any electronic system performing a cryptographic calculation involving a modular exponentiation, including a smart card 8 as [in the sole figure] shown in Fig. 1. The chip includes information processing means 9, connected on one end to a nonvolatile memory 10 and a volatile working memory RAM 11, and connected on another end to means 12 for cooperating with an information processing device. The nonvolatile memory 10 can comprise a non-modifiable ROM part and a modifiable part constituted by an EPROM, an EEPROM or a RAM of the "flash" type, or FRAM, (the latter being a ferromagnetic RAM)), i.e., having the characteristics of an EEPROM but with access times identical to those of a standard RAM.

For the chip, it is possible to use, in particular, a self-programmable microprocessor with a nonvolatile memory, as described in U.S. patent No. 4,382,279 [in the name of the Applicant] assigned to the assignee of the present invention. In a variant, the microprocessor of the chip is replaced, or at least supplemented, by logical circuits installed in a semiconductor chip. In essence, such circuits are capable of performing calculations, including authentication and signature calculations, as a result of hard-wired, rather than microprogrammed, electronics. In particular, they can be of the ASIC ("Application Specific Integrated Circuit") type. Advantageously, the chip is designed in monolithic form.

The following are the amended claims marked up to show the changes with underlining and bracketing:

1 1. (Amended) [Method] A method for protecting an electronic system
2 implementing a cryptographic [calculation] process involving calculation of a
3 modular exponentiation of a quantity (x), said modular exponentiation using a
4 secret exponent (d), [characterized in that] comprising breaking down said secret
5 exponent [is broken down] (d) [in to] into a plurality of k unpredictable values (d_1 ,
6 d_2 , ..., d_k), the sum of which is equal to said secret exponent.

1 2. (Amended) [Method] A method according to claim 1, characterized
2 in that said unpredictable values (d_1 , d_2 , ..., d_k), are obtained [in the following
3 way] by:

4 a) deriving ($k-1$) values [are obtained] by means of a random
5 generator; and

6 b) taking [the final value is obtained from] the difference between the
7 secret exponent and the ($k-1$) values to derive a final value.

1 3. (Amended) [Method] A method according to claim 1,
2 [characterized in that the] wherein calculation of the modular exponentiation is
3 performed [in the following way] by:

4 a) [for each of said k values,] raising the quantity (x) [is raised] by an
5 exponent comprising said value [in order] to obtain [a result,] a set of results
6 [thus being obtained] for each of said k values; and

7 b) calculating a product of the results obtained in step a) [is
8 calculated].

1 4. (Amended) [Method] A method according to claim 1,
2 [characterized in that] wherein at least one of said $(k-1)$ values is obtained by
3 means of a random generator and has a length [greater than or] at least equal to
4 64 bits.

1 5. (Amended) [Utilization of] Utilizing the method according to claim 1
2 in a smart card comprising information processing means.

1 6. (Amended) [Utilization of] Utilizing the method according to claim 1
2 [to protect] for protecting a cryptographic calculation process using the RSA
3 algorithm.

1 7. (Amended) [Utilization of] Utilizing the method according to claim 1
2 [to protect] for protecting a cryptographic calculation process using the Rabin
3 algorithm.